Filing and Security

b6
b7C

Primary Case: 288A-CG-118108

Case Title: (U) [redacted] NEAR NORTH INSURANCE COMPUTER INTRUSION-OTHER

Serial Number: 18

Serialized: 05/17/2002

Category: Full Investigation
Initiated: 05/14/2002

Details

Serial #: 18

Type: FD302

From: CHICAGO

To: CHICAGO

Document Title: [redacted]

Approval Date: 5/17/2002

b6
b7C

Classification: U

Contents
05/18/2002
[redacted], date of birth [redacted] social security account number [redacted] and [redacted] social security account number [redacted] were interviewed at their place of employment, KEMPER INSURANCE COMPANIES, 1 Kemper Drive, C- 3, Long Grove, Illinois, telephone number [redacted]. After being advised of the identities of the interviewing agents and the nature of the interview, [redacted] provided the following information: [redacted] stated that [redacted] worked at KEMPER INSURANCE COMPANIES, hereafter referred to as KEMPER, [redacted]

b6
b7C

[redacted] stated KEMPER does not implement a background check on consultants because the consulting company is supposed to do the background check. [redacted] stated KEMPER has minimal information about individual contract employees. [redacted] stated on or about 04/22/2002 he received a telephone call from representatives of NEAR NORTH INSURANCE BROKERAGE (NNIB), hereafter referred to as NNIB, who informed him that someone was accessing their network without authorization from an Internet Protocol (IP) address assigned to

KEMPER. [redacted] stated the individuals from NNIB with whom he spoke advised they had a strong suspicion of the identity of the intruder. [redacted] stated NNIB provided IP addresses and that [redacted] confirmed the IP addresses as belonging to KEMPER. [redacted] stated he asked KEMPER's Information Technology (IT) personnel to identify any links to NNIB's network from KEMPER's system and the individual most likely to have been at the specific KEMPER terminals used to access NNIB's network. [redacted] stated KEMPER's IT personnel identified [redacted] as the individual assigned to the intruder terminals. [redacted] stated KEMPER would have immediately terminated [redacted] but NNIB personnel requested KEMPER personnel "keep an eye" on [redacted] to monitor his activities more closely. [redacted] stated KEMPER personnel became uncomfortable with keeping [redacted] employed. [redacted] stated personnel from KROLL INC., a forensic computer investigation firm, were hired to handle the investigation regarding [redacted] s activities. [redacted] stated staff from KROLL who interviewed [redacted] advised KEMPER personnel that [redacted] did not seem to appreciate the gravity of the situation. [redacted] stated [redacted] advised the KROLL personnel that his intrusion into NNIB's network was strictly to satisfy his own curiosity and because he still had friends who worked at NNIB. [redacted] stated [redacted] was terminated at approximately 6:00 p.m on 04/24/2002 by KROLL personnel and [redacted] stated while employed at KEMPER, [redacted] was asked by the interviewing agents for the name of KEMPER's Internet service provider. [redacted] stated he would find out who provided Internet access to KEMPER and provide that information to the agents.

b6
b7C

[redacted]

b6
b7C
b7E

access of NNIB's network were implemented from four computer terminals at KEMPER. [redacted] stated three of the terminals belonged to KEMPER while the fourth terminal was [redacted] s personal laptop computer. [redacted] stated the most activity was perpetuated from [redacted] s personal laptop. [redacted] stated [redacted] allowed KROLL personnel to review his laptop computer prior to being terminated but that they did not find anything that pertained to the access of NNIB's network. [redacted] stated [redacted] declined to allow KROLL personnel to retain his laptop [redacted] stated the KEMPER network has a banner message that advised anyone using the system that all property, e-mail messages, etc., are the property of KEMPER. [redacted] stated that employees do not sign a written document acknowledging this policy. [redacted] stated KROLL personnel asked [redacted] if he did anything to KEMPER's network, meaning an unauthorized access to KEMPER's system. [redacted] stated [redacted] advised that he did not do anything to KEMPER's network. [redacted] stated there was no evidence that [redacted] accessed or hacked their computer network. [redacted] stated [redacted] handwrote a letter of apology to KEMPER management the same night he was interviewed and eventually terminated. [redacted] stated [redacted] advised he was also going write a letter of apology to NNIB regarding the situation. [redacted] stated the name of KEMPER's contact at KROLL who led the [redacted] investigation is [redacted] [redacted] telephone number [redacted] provided to the agents a copy of

b6
b7C

b6
b7C

b6
b7C

[redacted] handwritten apology letter to KEMPER regarding the situation, three images of hard drives from KEMPER computer terminals used by [redacted] to access NNIB's network, a letter from KROLL regarding their imaging of the three hard drives and a CD-ROM containing log files. [redacted] stated KEMPER has retained log files from early March 2002 through 04/20/2002. An FD-597 Receipt of Property was completed and a copy was provided to [redacted] The original FD-597 was placed in a 1-A envelope and secured in the case file. b6 b7C

Indexing

No Entities to display.

Intelligence

Potential IIR/SIR? No
Sentinel Tags: No Sentinel Tags Selected

Can you identify the source of this information? No

Routing

Drafted By:

Approved By:

b7E

Filing and Security

b6
b7C

Primary Case: 288A-CG-118108

Case Title: (U) NORTH INSURANCE COMPUTER INTRUSION-OTHER

Serial Number: 19

Serialized: 05/17/2002

Category: Full Investigation
Initiated: 05/14/2002

Details

Serial #: 19

Type: FD302

From: CHICAGO

To: CHICAGO

Document Title:

b6
b7C

Approval Date: 5/17/2002

Classification: U

Contents 05/29/2002

date of birth was interviewed at his place of employment, KEMPER INSURANCE COMPANIES, 1 Kemper Drive, Long Grove, Illinois, telephone number . After being advised of the identities of the interviewing agents and the nature of the interview, provided the following information: was asked how Internet traffic leaving KEMPER's location and directed to NEAR NORTH INSURANCE BROKERAGE (NNIB) would be routed via the Internet stated Internet traffic would be routed through KEMPER's server at the Long Grove, Illinois location and directly to NNIB's server in Chicago, Illinois. stated as it pertains to Internet traffic directed to NNIB, he did not observe a KEMPER server location from outside Illinois receiving Internet traffic stated he observed that four work stations at KEMPER were used to access NNIB's e-mail server, stated three of the locations belonged to KEMPER and one station was assigned to a laptop computer belonging to stated when was interviewed by and KROLL INC. personnel regarding his unauthorized access of NNIB's network, would not let KROLL or KEMPER personnel image the hard drive contained in his laptop. stated he and the KROLL personnel had the laptop for approximately 45 minutes. stated KEMPER e-mail account contained no suspicious activity, stated he suspended any dial-in and VPN access belonging to stated had no accounts on KEMPER's mainframe system, stated KEMPER has three Internet Protocol ranges all beginning with the number "198". stated KEMPER implements the intrusion detection software manufactured by ISS called Real Secure.

b6
b7C

b6
b7C